Open letter to UN General Assembly: Proposed international convention on cybercrime poses a threat to human rights online

Excellencies,

Countering cybercrime is a key challenge that requires international cooperation. However, the approach taken in the draft resolution “Countering the use of information and communications technologies for criminal purposes” (A/C.3/74/L.11/Rev.1) at the UN General Assembly (UNGA) Third Committee is fundamentally flawed and would restrict the use of the internet for human rights, and social and economic development. **The undersigned organisations urge your delegation to vote against the draft resolution**.

The resolution would “establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.” We are not convinced that there is a need for a new international convention on cybercrime. We have grave concerns that the approach for the UN's work in this area proposed in the “Draft United Nations Convention on Cooperation in Combating Cybercrime” (A/C.3/72/12), circulated by the Russian Federation, could undermine the use of the internet to exercise human rights and facilitate social and economic development.

Our concerns with the resolution and the process it initiates are as follows:

First, the “use of information and communications technologies for criminal purposes” is not defined in the resolution. The text includes both cybersecurity issues (crimes that impact the “stability of critical infrastructure of States and enterprises”) as well as criminal acts that are enabled through ICTs (for example, “traffickers in persons [...] taking advantage of information and communications technologies to carry out criminal activities”). The lack of specificity is not just a concern from an accuracy perspective; keeping the term undefined opens the door to criminalising ordinary online behaviour that is protected under international human rights law.

Second, criminalising ordinary online activities of individuals and organisations through the application of cybercrime laws constitutes a growing trend in many

countries in the world. The UN Special Rapporteur on the rights to freedom of peaceful assembly and of association has observed: “A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world.”[1] As his report notes, such laws are used to criminalise access to and use of secure digital communications (through, for example, the use of encryption), which are vital to the work of civil society, human rights defenders (HRDs) and journalists, as well as public and private institutions that rely on a stable and secure internet; to criminalise legitimate forms of online expression, association and assembly through vague and ill-defined terms that allow for arbitrary or discretionary application and resulting in legal uncertainty; and to give wide-ranging power to governments to block websites deemed critical of the authorities, or even entire networks, applications and services that facilitate online exchange of and access to information.

While legislation aimed at addressing cybercrime can be necessary and reinforce democratic institutions, when misused, cybercrime laws can create a chilling effect and hinder people’s ability to use the internet to exercise their rights online and offline. As various UN Special Procedures have raised in communications with governments, cybercrime laws can result in arbitrary arrests, detention, and even death.[2] The one reference to human rights included in the draft resolution, simply reaffirming the importance of respect for human rights and fundamental freedoms in the use of ICTs, is insufficient to safeguard human rights while countering cybercrime.

1 2019 Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (A/HRC/41/41)

2 Saudi Arabia (SAU 13/2014) Communication from the Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression; freedom of religion or belief; and on the situation of human rights defenders on the sentencing of Mr. Raef Badawi on charges of “insulting Islam” under Anti-Cyber Crime Law; Bangladesh (BGD 14/2013) Communication from the Working Group on Arbitrary Detention, and the Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression; the rights to freedom of peaceful assembly and of association; and on the situation of human rights defenders on the situation of Mr. Nasiruddin Elan, Director of Odhikar, a non-governmental organization, who was arrested for allegedly violating Section 57 of the Information and Communications Technology Act and brought before the Cyber Crimes Tribunal; UAE (ARE 5/2013) Communication from Special Rapporteurs on the promotion and protection of the right to freedom of opinion and expression; the rights to freedom of peaceful assembly and of association; on the situation of human rights defenders; and on torture and other cruel, inhuman or degrading treatment or punishment on the alleged use of the new Cyber Crime Law to impose undue restrictions on online freedom of expression; Iran (IRN 27/2012) Communication from the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the situation of human rights defenders; the Special Rapporteur on the situation of human rights in the Islamic Republic of Iran; the Special Rapporteur on extrajudicial, summary or arbitrary executions; and the Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment on the alleged torture resulting in the death of Sattar Beheshti while in custody after being arrested on cybercrime related charges.

Third, the "Draft United Nations Convention on Cooperation in Combating Cybercrime", which is meant to serve as a basis for developing a comprehensive international convention, raises a number of concerns. Of particular concern is that the Draft Convention proposes going far beyond what the Budapest Convention allows for regarding cross-border access to data, including by limiting the ability of a signatory to refuse to provide access to requested data.[3] The Draft Convention would also establish the UN as the enforcement point, by creating an International Technical Commission on Combating ICT Crime as a UN organ, among other enforcement mechanisms. A number of provisions in the Draft Convention echo those of the Budapest Convention; however, references to balancing the interests of law enforcement and respect for fundamental human rights are absent, as are references to the principle of proportionality and to due process rights. Given the Russian Federation's efforts to expand government control over the internet, with the so-called "sovereign internet" law going into effect earlier this month,[4] its leadership in developing an international binding treaty on cybercrime deserves high levels of scrutiny.

Fourth, we are not convinced that there is a need for a new international convention on cybercrime. Building on and improving existing instruments is more desirable and practical than diverting already scarce resources into the pursuit of a new international framework, which is likely to stretch over many years and unlikely to result in consensus. There is already work being done in other parts of the UN to address cybercrime, specifically by the UN Office on Drugs and Crime (UNODC), as well as at the national and regional levels. According to the UNODC database on cybercrime legislation, over 180 countries have substantive and procedural legislation on cybercrime and electronic evidence.[5] Certainly there are challenges in terms of the varying strength of national laws, as well as the capacity of national governments to implement them; however, there is already a UN process working to address this. The UN Open-ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime is expected to release its report in 2021, which should include its findings and recommendations on national legislation, best practices, technical assistance and international cooperation.[6] There is currently a process underway to develop a Second Additional Protocol to the Budapest Convention, which is the most

3 Articles 51-56 of the Draft Convention establish conditions for the availability of data from other states. While they do not go so far as to say that all states would be forced to turn over all relevant information, these articles put a strong degree of pressure to do so on all signatories by requiring that domestic law be modified to support turnover of traffic and content data under the conditions defined in the convention and the licences agreed upon by the states.

4 https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online

5 The database contains extracts of laws relevant to cybercrime offences and cross-cutting issues and allows users to access full legislation documents.

6 https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2019.html

widely ratified international instrument on cybercrime.[7]

Finally, countering cybercrime is necessarily a multistakeholder endeavour. It requires government officials and experts, members of the technical community, civil society, the private sector, and scientific and research institutions. The establishment of an ad hoc intergovernmental committee of experts to address the issue of cybercrime would exclude key stakeholders who bring valuable expertise and perspectives both in terms of effectively countering the use of ICTs for criminal purposes and to ensure that such efforts do not undermine the use of ICTs for the enjoyment of human rights and social and economic development.

We strongly urge your delegation to vote against resolution A/C.3/74/L/11/Rev.1 on "Countering the use of information and communications technologies for criminal purposes" and to work to ensure that initiatives to address cybercrime are inclusive of all stakeholders.

Yours sincerely,

7amleh - The Arab Center for the Advancement of Social Media
Access Now
Africa Freedom of Information Centre
Albanian Media Institute
Americans for Democracy & Human Rights in Bahrain
ARTICLE 19
Association for Progressive Communications (APC)
Bangladesh NGOs Network for Radio and Communication
BlueLink – Bulgaria
Bytes for All (B4A) – Pakistan
Child Rights International Network (CRIN)
Derechos Digitales – Latin America
Digital Rights Foundation
Electronic Frontier Foundation (EFF)
eQuality Project, University of Ottawa – Canada
Fundación Huaira – Quito, Ecuador
Fundación Internet Bolivia
Global Partners Digital
Hiperderecho – Peru
Human Rights in China

7Civil society is engaging in the development of the Second Additional Protocol to the Budapest Convention in an effort to address some of the Convention's shortcomings, in particular by ensuring that requests for personal data across borders comply with human rights protections. https://www.eff.org/document/joint-civil-society-response-discussion-guide-2nd-additional-protocol-budapest-convention

Internet Governance Project
Internet Policy Observatory – Pakistan
Internet Society
IPANDETEC – Central America
Jonction – Senegal
Media Institute of Southern Africa (MISA)
Media Matters for Democracy – Pakistan
Paradigm Initiative – Nigeria
Privacy International
Red en Defensa de los Derechos Digitales (R3D)
Research ICT Africa
Software Freedom Law Center
TEDIC – Paraguay
Usuarios Digitales
Vigilance for Democracy and the Civic State – Tunisia
YMCA Computer Training Centre and Digital Studio – The Gambia

Individuals:

(Affiliations listed for purposes of identification)

Dr. Jennifer Barrigar
Canada

Tamir Israel
Staff lawyer, Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)

Douwe Korff
Emeritus Professor of International Law, London Metropolitan University and Associate of the Oxford Martin School, University of Oxford.

Joy Liddicoat
Researcher, University of Otago, New Zealand and Vice President at InternetNZ

Damian Loreti
University of Buenos Aires, Argentina

Valerie Steeves
Full Professor, Department of Criminology, University of Ottawa, Canada